

THIS DOCUMENT IS NOT A CONTRACT OF EMPLOYMENT. PRIOR DOCUMENTS ON THIS SUBJECT ARE REVOKED. EMPLOYMENT WITH THE CITY OF GREENVILLE IS AT-WILL.

CITY OF GREENVILLE

POLICY NO.: HR-30

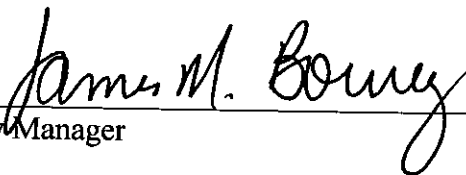
DATE: December 14, 2005

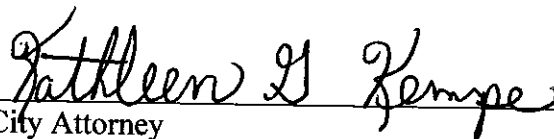
SUBJECT: Internet and Email Usage

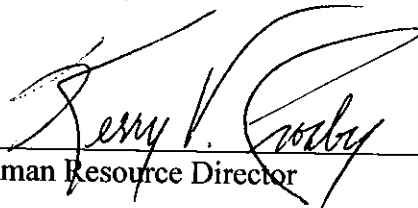
CONTENTS

- I. Purpose
- II. Scope
- III. Policy
- IV. Procedures

APPROVALS:


City Manager


City Attorney


Human Resource Director

I. Purpose

To provide regulations to City of Greenville personnel in their workplace use of the internet and email systems (and any other means of electronic communication).

II. Scope

This policy specifies the proper utilization of email and internet access as well as the computer facilities and services ("hardware" and "software") owned or leased by the City of Greenville (the City), or otherwise licensed to the City, through which email and internet access is accomplished (hereinafter called "computer services.") These facilities include, but are not limited to: PCs (personal computers), all components inside a PC, all components connected to a PC, monitors, printers, display stations, servers, telephones, hubs, switches, routers, cabling, mobile data terminals, personal digital assistants and handheld computers (operating as a stand-alone system or connected through a wired or wireless network), all software applications and operating systems, all data, all data lines, all phone lines, wireless communications facilities, etc and all files prepared by City employees or received by City employees when using the City's computer services.

This policy applies to all employees, contractors, part-time employees, volunteers, and other individuals who are granted access to City of Greenville's computer services (hereinafter called "computer users" or "users"). This policy is intended to ensure that all City computer users understand their responsibilities in regards to proper usage of the City's computer services.

The City's computer services are made available to users for City business and are not provided for the purpose of facilitating private or personal communications or file preparation. Use of the City's computer services is not an entitlement. It is an opportunity which carries with it responsibilities.

Employees entrusted with the use of the City's computer services must be held accountable for the proper use of the facilities. All users granted access privileges with City of Greenville computer services are required to comply with this policy. This policy must be read in conjunction with other City policies including, but not limited to, those regarding City communications, confidentiality, solicitation, harassment, discrimination, etc.

III. Policy

A. Internet and email access is provided to City users to facilitate and expedite communications and research necessary for the conduct of City business. The City encourages the use of email and internet access for that purpose. The computer services needed to provide email and internet access represent a considerable financial commitment by the City for telecommunications, networking, software, storage,

support, etc. The City intends for this tool to be used in a responsible, efficient, ethical, professional, and legal manner, consistent with the City's business needs.

- B. All data and messages originating from, received at or transmitted through the City's computer services are the property of City of Greenville.
- C. Subject to the mandates and objectives of this policy, brief personal use of internet and email systems is permitted if it does not:
 - 1. Interfere with one's work or anyone else's work at the City;
 - 2. Have a harmful effect on the performance of City computer services, such as when internet browsers and applications are left open for extended periods of time or when software unrelated to City business is downloaded;
 - 3. Violate or infringe upon the right of any other person or entity in the lawful exercise of their rights and duties;
 - 4. Constitute a criminal offense or give rise to civil liability; or
 - 5. Violate a City policy or regulation.

Systematic and pervasive use of email or internet systems for non-job-related purposes is strictly prohibited.

- D. Electronic exchanges that occur in the course of conducting City business will be considered a communication of the City and will be held to the same standards as formal letters. Email messages are considered business records which are subject to discovery in administrative, judicial, and other legal proceedings. Email messages, whether sent or received, are subject to Requests for Information from any member of the public under the Freedom of Information Act.
- E. Personal email messages are not private, despite any contrary designation by the sender or the recipient. Accordingly, computer users can have no reasonable expectation of privacy in using the City's computer services in the transmission and receipt of internet information and email messages.
- F. Email messages sent or received in the conduct of City business are not confidential unless they qualify for non-disclosure under the Freedom of Information Act and then only to the extent permitted under the Act.
- G. Inappropriate use of the City email system and internet access is prohibited. Such inappropriate uses include, but are not limited to, the following:
 - 1. Reading or sharing information via the email system without proper authorization.
 - 2. Developing web or home pages for personal use;

3. Broadcasting unsolicited messages to internal or external email addresses, unless authorized by a division or department head as a means of official notice for City business;
4. Sending large and/or useless files to random users;
5. Broadcasting unsolicited pyramid or chain email;
6. Committing any crime using the internet;
7. Making threats against other persons or institutions;
8. Mounting an attack on the security of any system, including attempts to hack into or to introduce or spread viruses through a system,
9. Using obscene or pornographic language, pictures, or drawings in outgoing mail or willfully receiving files containing obscene or pornographic language, pictures, or drawings, regardless of whether such files are downloaded, except for police officers working on a criminal case where such information is related to that criminal case. Attachments to email messages containing such language or pictures are also prohibited;
10. Using any language or subject matter, which if spoken or written, would constitute unacceptable behavior in the work place, including harassing, discriminatory, offensive, hostile, suggestive, defamatory, or otherwise inappropriate language;
11. Participating in online publishing activities or in online discussion groups that are not work related;
12. Downloading files in such a way as to avoid copyright infringement;
13. Loading and accessing personal internet provider accounts (e.g., America On Line, etc.);
14. Sharing email and internet passwords or gaining access, without permission, to another employee's email or internet access.
15. Disguising one's identity in any way, including the sending of falsified messages.
16. Offering personal products or services for sale, soliciting for outside business ventures, personal parties, membership in any organization, political causes, religious causes, social causes, soliciting funds for charities without approval or other matters not connected to the City's business.
17. Using email in lieu of an employee's responsibility to contact his/her immediate supervisor directly for the purpose of reporting that an individual is unable to work on a given day.
18. Intercepting, recording, reading, altering, or receiving another person's email messages, when doing so is not part of one's job performance, unless authorized by the appropriate department head.
19. Using the City's computer services in any way prohibited by City of Greenville policies or procedures.

IV. Procedures

A. Office of Management and Budget

1. The City reserves the right to monitor and record all messages of all City computer services and has empowered the Office of Management and Budget (OMB) to monitor each employee's internet and email usage on a random and unannounced basis to confirm compliance with the City's policy. The Director of the Office of Management and Budget will designate an individual to coordinate the monitoring and reporting function.
2. The City reserves the right to inspect any and all files stored on computer facilities in order to assure compliance with this policy.
3. The City uses security software that is capable of recording each and every internet website visit, each chat, newsgroup or email message, and each file transfer into and out of the City's internal networks, and the City reserves the right to utilize this software at any time. The City's security software can record internet activity and analyze usage patterns. When patterns of inappropriate activity are observed, a written report of the activity will be made available to the department head of the person whose computer and network login is associated with the activity.
4. If OMB, during the course of monitoring internet and email activity, detects usage that appears to violate local, State or Federal law, a written report of such usage will be provided to an officer of the Greenville Police Department who is designated by the Police Chief to receive and investigate such reports. A copy of the written report will also be provided to the Human Resources Director and/or the City Manager.
5. OMB will provide standard internet usage reports to all department heads and, upon the request of a department head, will monitor and provide reports on internet and email system usage by individual employees and groups of employees in the department of the requesting department head.
6. OMB, upon the request of the Human Resources Director, City Attorney or City Manager, will monitor and provide reports on internet and email system usage by individual employees and groups of employees in any department.
7. OMB will educate internet and email system users to avoid practices that violate City policy or applicable local, State or Federal law or which will detract from internet connection performance.
8. OMB is authorized to terminate internet and email privileges for any account that has not been utilized in 90 calendar days.
9. OMB is authorized to set prudent operating standards and to make periodic adjustments in operating procedures for computer services, as needed, to maximize system capacity, security and performance. OMB will publicize such adjustments via email and by other means.

B. Users of Computer Services

1. Users of City owned computer services are personally responsible and accountable for all material received and sent through their accounts or user

identification, including mail, data, documents, and software. Thus, users are encouraged to password-protect access to computer services while absent from their work area during normal business hours. After normal business hours, computers must be logged out to avoid unauthorized persons from accessing the computer. (The purpose of this provision is to protect official information from unauthorized or premature inspection in those instances when policies, practices, and programs are in a developmental stage; when personnel information is under review; when investigations are underway; when proprietary information has been transmitted, prepared or assessed or in other like circumstances requiring the orderly preparation and transmission of information.)

2. Users must refrain from leaving non-business related web pages open and unattended for extended period of time and to refrain from accessing internet websites or applications which consume large amounts of computer resources. Such applications include streaming video and audio.
3. Users of computer services must understand that email is the preferred vehicle with which lawbreakers transmit destructive viruses, and thus users must use extreme caution when opening email attachments, even when email attachments come from trusted sources. Any computer user who receives a suspicious email attachment should not open the attachment, but should delete the email or contact the Help Desk for assistance.
4. Users must understand that the use of the email "delete" function does not immediately remove the targeted message from the City's email server. Messages deleted from the email system may still be available to others, either through a system backup or from all recipients of the message.
5. To more effectively manage city computer resources, users are expected to comply with periodic OMB advice and directives related to computer services, such as login/logoff procedures, avoiding internet websites and applications that overtax City computer services, archiving historical emails and deleting emails with large-size file attachments.
6. If the employment of any user is discontinued, that user has no rights to the content of his/her email messages unless authorized by the Division head, department head or City Manager. The person will not be allowed further access to the City email system. Thus, a change in employment status may cause an individual to lose authorization to the City email system. Changes in employment status include, but are not limited to: resignation, retirement, termination, reassignment, promotion, demotion, or a loss of authorized user status. If such a change in employment status occurs, the Human Resources Department will notify designated person(s) in OMB so that OMB can remove email privileges for the affected person. However, OMB will only delete an individual's email after receiving approval of the employee's department head.

C. Other Personnel

1. The Human Resources Director and designated persons in the Police Department are responsible for further investigation and follow-up on reported internet and email activity that appears to be illegal.
2. The Human Resources Department will notify designated person(s) in OMB of employee status changes that require removal of internet and email privileges so that OMB can remove email privileges for the affected person.
3. Department heads are responsible for distributing this policy to all affected employees in their departments, organizing training on the policy, as appropriate and enforcing compliance with the policy.
4. Department heads or their designees may request and be granted access to an employee's computer account if the employee is on leave of absence or vacation, is transferred or terminated, or any time when there is a valid business justification.
5. The Human Resources Director, City Attorney or City Manager may request OMB to monitor and provide reports on internet and email system usage by individual employees and groups of employees in any department.
6. Department heads may request OMB to monitor and provide reports on internet and email system usage by individual employees and groups of employees in the department of the requesting department head.

D. Violations of this policy may result in disciplinary action. This action may include, but is not limited to, loss of internet access and email privileges, probation, suspension, termination of employment and/or civil or criminal penalties. In the event possible illegal activity is discovered, the City will cooperate with any legitimate law enforcement authority.

E. Exceptions to this policy may be granted on a case-by-case basis, upon request by department head and approval by the City Manager.

F. The City reserves the right to modify this policy at any time.